Manifest configurations

- [ ] Check for backup set to true
- [ ] Check if permission write to external storage is set - review that no sensitive data is stored there
- [ ] Check if application is running in debuggable mode
- [ ] Check if network security cleartextpermitted is set to true.

Components

Activities

- [ ] Check for exported activities
- [ ] Check for hidden exported activities
- [ ] Check for interesting views, usable in highly unlikely and ridiculous phishing attack
- [ ] Check for activities that take arguments, and if those arguments do something interesting.

Content providers

- [ ] Check if content providers are exported
- [ ] Check if sensitive information can be accessed
- [ ] Check for sql injection

Services

- [ ] Check if servies are exported
- [ ] Check to see if you can interact with the service

Broadcast

- [ ] Check if broadcasts are exported

Storage

- [ ] Check for world readable files in the app
- [ ] Check for sensitive information in shared_prefs
- [ ] Check for unencrypted sensitive files in SQL database

Unintended data leaks

- [ ] Disallow copy-paste for sensitive data
- [ ] Analytics sent to third party
- [ ] Check that sensitive data is not logged
- [ ] Check for Firebase access control

WebView attacks

- [ ] Check that Javascript if disabled

Network security

- [ ] Check for unencrypted HTTP traffic
- [ ] Check for non-http traffic
- [ ] Check if application verifies server certificate

Misc

- [ ] Check for hardcoded credentials
- [ ] TEMP: Act if mobile is rooted